WHAT IS CLAIMED IS:

1. A contents distribution method through the use of a communication network over which a recipient machine, an entitlement granter machine, and a contents distributor machine are interconnected, comprising:

a step to be taken on the recipient machine that is sending a message containing contents request information that the recipient wants to get specific contents to the entitlement granter machine;

a step to be taken on the entitlement granter machine that comprises sequential actions of encrypting digital rights data relevant to the contents request information with the recipient's public key, putting digital signature using the entitlement granter's secret key to the thus encrypted digital rights data, and sending the encrypted digital rights data with the entitlement granter's digital signature thereon to the recipient machine;

a step to be taken on the recipient machine that comprises sequential actions of decrypting the encrypted digital rights data with the recipient's secret key and sending a message containing digital rights data thus decrypted and the encrypted digital rights data with the entitlement granter's digital signature thereon to the contents distributor machine;

a step to be taken on the contents distributor machine that comprises sequential actions of verifying the entitlement granter's digital signature by using the entitlement granter's public key, encrypting the digital rights data with the recipient's public key, making sure that the thus encrypted digital rights data matches with the encrypted digital rights data, encrypting contents data to be sent to the recipient machine with the recipient's public key, and sending the thus encrypted contents data to the recipient machine; and

a step to be taken on the recipient machine that is decrypting the encrypted contents data with the recipient's secret key.

2. A contents distribution method through the use of a communication network over which a recipient machine, an entitlement granter machine, and a contents distributor machine are interconnected, comprising:

a step to be taken on the recipient machine that is sending a message containing the recipient's public key and contents request information that the recipient wants to get specific contents to the entitlement granter machine;

a step to be taken on the entitlement granter machine that comprises sequential actions of encrypting digital rights data relevant to the contents request information

with the recipient's public key, putting digital signature using the entitlement granter's secret key to the thus encrypted digital rights data, and sending the encrypted digital rights data with the entitlement granter's digital signature thereon to the recipient machine;

a step to be taken on the recipient machine that comprises sequential actions of decrypting the encrypted digital rights data with the recipient's secret key and sending a message containing digital rights data thus decrypted, the encrypted digital rights data with the entitlement granter's digital signature thereon, and the recipient's public key to the contents distributor machine;

a step to be taken on the contents distributor machine that comprises sequential actions of verifying the entitlement granter's digital signature by using the entitlement granter's public key, encrypting the digital rights data with the recipient's public key, making sure that the thus encrypted digital rights data matches with the encrypted digital rights data, encrypting contents data to be sent to the recipient machine with the recipient's public key, and sending the thus encrypted contents data to the recipient machine; and

a step to be taken on the recipient machine that is decrypting the encrypted contents data with the recipient's secret key.

3. The contents distribution method according to claim 1, further comprising:

a step of sending an entry form for acquiring information about the recipient from the contents distributor machine to the recipient machine after the action of making sure of encrypted digital rights data matching is carried out on the contents distributor machine;

a step to be taken on the recipient machine that comprises sequential actions of generating an entry form filled with data as a result of that the recipient enters necessary information into the entry form, putting digital signature using the recipient's secret key to the entry form filled with data, and sending the entry form filled with data with the recipient's digital signature thereon to the contents distributor machine; and

a step to be taken on the distributor machine that comprises sequential actions of verifying the recipient's digital signature by using the recipient's public key and sending the contents data encrypted with the recipient's public key to the recipient machine.

4. The contents distribution method according to claim 2, further comprising:

a step of sending an entry form for acquiring information about the recipient from the contents distributor machine to the recipient machine after the action of making sure of encrypted digital rights data matching is carried out on the contents distributor machine;

a step to be taken on the recipient machine that comprises sequential actions of generating an entry form filled with data as a result of that the recipient enters necessary information into the entry form, putting digital signature using the recipient's secret key to the entry form filled with data, and sending the entry form filled with data with the recipient's digital signature thereon to the contents distributor machine; and

a step to be taken on the distributor machine that comprises sequential actions of verifying the recipient's digital signature by using the recipient's public key and sending the contents data encrypted with the recipient's public key to the recipient machine.

5. The contents distribution method according to claim 1, wherein:

when the entitlement granter machine sends the encrypted digital rights data to the recipient machine, a certificate that is objective authentication of the

entitlement granter and includes the entitlement granter's public key is attached to the data;

when the recipient machine sends the digital rights data to the contents distributor machine, the certificate of the entitlement granter is attached to the data; and

the contents distributor machine verifies the certificate of the entitlement granter and uses the entitlement granter's public key derived from the certificate of the entitlement granter when verifying the entitlement granter's digital signature.

6. The contents distribution method according to claim 2, wherein:

when the entitlement granter machine sends the encrypted digital rights data to the recipient machine, a certificate that is objective authentication of the entitlement granter and includes the entitlement granter's public key is attached to the data;

when the recipient machine sends the digital rights data to the contents distributor machine, the certificate of the entitlement granter is attached to the data; and

the contents distributor machine verifies the certificate of the entitlement granter and uses the entitlement granter's public key derived from the

certificate of the entitlement granter when verifying the entitlement granter's digital signature.

7. The contents distribution method according to claim 3, wherein:

when the entitlement granter machine sends the encrypted digital rights data to the recipient machine, a certificate that is objective authentication of the entitlement granter and includes the entitlement granter's public key is attached to the data;

when the recipient machine sends the digital rights data to the contents distributor machine, the certificate of the entitlement granter is attached to the data; and

the contents distributor machine verifies the certificate of the entitlement granter and uses the entitlement granter's public key derived from the certificate of the entitlement granter when verifying the entitlement granter's digital signature.

8. A contents distribution system having a recipient machine, an entitlement granter machine, and a contents distributor machine interconnected over a communication network, comprising:

a computer system built on the recipient machine and comprised of a means to send a message containing contents

request information that the recipient wants to get specific contents to the entitlement granter machine, a means to decrypt encrypted digital rights data sent from the entitlement granter machine with the recipient's secret key, a means to send a message containing digital rights data thus decrypted and the encrypted digital rights data with the entitlement granter's digital signature thereon to the contents distributor machine, and a means to decrypt encrypted contents data sent from the contents distributor machine with the recipient's secret key.

a computer system built on the entitlement granter machine and comprised of a means to encrypt digital rights data relevant to the contents request information with the recipient's public key, a means to put the entitlement granter's digital signature generated by using the entitlement granter's secret key to the thus encrypted digital rights data, and a means to send the encrypted digital rights data with the entitlement granter's digital signature thereon to the recipient machine; and

a computer system built on the contents distributor machine and comprised of a means to verify the entitlement granter's digital signature by using the entitlement granter's public key, a means to encrypt the digital rights data with the recipient's public key and make sure that the thus encrypted digital rights data matches with the

encrypted digital rights data, and a means to encrypt contents data to be sent to the recipient machine with the recipient's public key and send the thus encrypted contents data to the recipient machine.

9. A contents distribution system having a recipient machine, an entitlement granter machine, and a contents distributor machine interconnected over a communication network, comprising:

a computer system built on the recipient machine and comprised of a means to send a message containing the recipient's public key and contents request information that the recipient wants to get specific contents to the entitlement granter machine, a means to decrypt encrypted digital rights data sent from the entitlement granter machine with the recipient's secret key, a means to send a message containing digital rights data thus decrypted, the encrypted digital rights data with the entitlement granter's digital signature thereon, and the recipient's public key to the contents distributor machine, and a means to decrypt encrypted contents data sent from the contents distributor machine with the recipient's secret key.

a computer system built on the entitlement granter machine and comprised of a means to encrypt digital rights data relevant to the contents request information with the

recipient's public key, a means to put the entitlement granter's digital signature generated by using the entitlement granter's secret key to the thus encrypted digital rights data, and a means to send the encrypted digital rights data with the entitlement granter's digital signature thereon to the recipient machine; and

a computer system built on the contents distributor machine and comprised of a means to verify the entitlement granter's digital signature by using the entitlement granter's public key, a means to encrypt the digital rights data with the recipient's public key and make sure that the thus encrypted digital rights data matches with the encrypted digital rights data, and a means to encrypt contents data to be sent to the recipient machine with the recipient's public key and send the thus encrypted contents data to the recipient machine.

10. The contents distribution system according to claim 8, wherein:

the computer system built on the contents distributor machine is further comprised of a means to send an entry form for acquiring information about the recipient to the recipient machine after making sure of encrypted digital rights data matching;

the computer system built on the recipient machine is further comprised of a means to generate an entry form filled with data as a result of that the recipient enters necessary information into the entry form, put digital signature using the recipient's secret key to the entry form filled with data, and send the entry form filled with data with the recipient's digital signature thereon to the contents distributor machine; and

the computer system built on the contents distributor machine is further comprised of a means to verify the recipient's digital signature by using the recipient's public key and then send the contents data encrypted with the recipient's public key to the recipient machine.

11. The contents distribution system according to claim 9, wherein:

the computer system built on the contents distributor machine is further comprised of a means to send an entry form for acquiring information about the recipient to the recipient machine after making sure of encrypted digital rights data matching;

the computer system built on the recipient machine is further comprised of a means to generate an entry form filled with data as a result of that the recipient enters necessary information into the entry form, put digital signature using

the recipient's secret key to the entry form filled with data, and send the entry form filled with data with the recipient's digital signature thereon to the contents distributor machine; and

the computer system built on the contents distributor machine is further comprised of a means to verify the recipient's digital signature by using the recipient's public key and then send the contents data encrypted with the recipient's public key to the recipient machine.

12. The contents distribution system according to claim 8, wherein:

the means to send the encrypted digital rights data to the recipient machine, provided on the entitlement granter machine attaches a certificate that is objective authentication of the entitlement granter and includes the entitlement granter's public key to the data to send;

the means to send the digital rights data to the contents distributor, provided on the recipient machine attaches the certificate of the entitlement granter to the data to send; and

the means to verify the entitlement granter's digital signature, provided on the contents distributor machine verifies the certificate of the entitlement granter and uses the entitlement granter's public key derived from

the certificate of the entitlement granter when verifying the entitlement granter's digital signature.

13. The contents distribution system according to claim 9, wherein:

the means to send the encrypted digital rights data to the recipient machine, provided on the entitlement granter machine attaches a certificate that is objective authentication of the entitlement granter and includes the entitlement granter's public key to the data to send;

the means to send the digital rights data to the contents distributor, provided on the recipient machine attaches the certificate of the entitlement granter to the data to send; and

the means to verify the entitlement granter's digital signature, provided on the contents distributor machine verifies the certificate of the entitlement granter and uses the entitlement granter's public key derived from the certificate of the entitlement granter when verifying the entitlement granter's digital signature.

14. The contents distribution system according to claim 10, wherein:

the means to send the encrypted digital rights data to the recipient machine, provided on the entitlement

granter machine attaches a certificate that is objective authentication of the entitlement granter and includes the entitlement granter's public key to the data to send;

the means to send the digital rights data to the contents distributor, provided on the recipient machine attaches the certificate of the entitlement granter to the data to send; and

the means to verify the entitlement granter's digital signature, provided on the contents distributor machine verifies the certificate of the entitlement granter and uses the entitlement granter's public key derived from the certificate of the entitlement granter when verifying the entitlement granter's digital signature.

15. An entitlement granter machine connected to a recipient machine operated by a recipient who wants to get contents data across a network,

a computer system built on the entitlement granter machine being comprised of a means to receive a message containing contents request information that the recipient want to get specific contents from the recipient machine, a means to encrypt digital rights data relevant to the contents request information with the recipient's public key, a means to put the entitlement granter's digital signature generated by using the entitlement granter's

secret key to the thus encrypted digital rights data, and a means to send the encrypted digital rights data with the entitlement granter's digital signature thereon to the recipient machine.

16. An entitlement granter machine connected with a recipient machine operated by a recipient who wants to get contents data across a network,

a computer system built on the entitlement granter machine being comprised of a means to receive a message containing contents request information that the recipient want to get specific contents and the recipient's public key from the recipient machine, a means to encrypt digital rights data relevant to the contents request information with the recipient's public key, a means to put the entitlement granter's digital signature generated by using the entitlement granter's secret key to the thus encrypted digital rights data, and a means to send the encrypted digital rights data with the entitlement granter's digital signature thereon to the recipient machine.

17. The entitlement granter machine according to claim 15, wherein:

the computer system built on the entitlement granter machine is further comprised of a means to extract

digital rights data that has been put under management beforehand, based on the contents request information.

18. A contents distributor machine connected with a recipient machine across a network,

a computer system built on the contents distributor machine being comprised of a means to receive digital rights data relevant to contents request information, encrypted digital rights data generated by encrypting the digital rights data with the recipient's public key, and the entitlement granter's digital signature put to the encrypted digital rights data, a means to verify the entitlement granter's digital signature by using the public key of the entitlement granter, a means to encrypt the digital rights data with the recipient's public key and make sure that the thus encrypted digital rights data matches with received encrypted digital rights data, a means to encrypt contents data to be sent to the recipient machine with the recipient's public key, and a means to send the thus encrypted contents data to the recipient machine.

19. A contents distributor machine connected with a recipient machine across a network,

a computer system built on the contents distributor machine being comprised of a means to receive digital rights

data relevant to contents request information, encrypted digital rights data generated by encrypting the digital rights data with the recipient's public key, the entitlement granter's digital signature put to the encrypted digital rights data, and the recipient's public key, a means to verify the entitlement granter's digital signature by using the public key of the entitlement granter, a means to encrypt the digital rights data with the recipient's public key and make sure that the thus encrypted digital rights data matches with received encrypted digital rights data, a means to encrypt contents data to be sent to the recipient machine with the recipient's public key, and a means to send the thus encrypted contents data to the recipient machine.

20. The contents distributor machine according to claim 19, wherein:

the computer system built on the contents distributor machine is further comprised of a means to send an entry form for acquiring information about the recipient to the recipient machine and a means to receive the entry form filled with data with the recipient's digital signature encrypted with the recipient's secret key thereon if the match between the digital rights data encrypted with the recipient's public key and the received encrypted digital rights data has been verified; and

a means to encrypt contents data to be sent to the recipient machine with the recipient's public key if the validity of the recipient's digital signature put to the received form has been verified by using the recipient's public key.